Contemporary Engineering Sciences, Vol. 9, 2016, no. 13, 627 - 633
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2016.6450

A Comparative Analysis of Personal Data Protection Policies of Leading Countries in the Internet of Things (IoT) Environment

Kyoungsik Min

Korea Internet & Security Agency
IT Venture Tower, Songpa-gu, Seoul, Korea

Seung-Woan Chai

Korea Internet & Security Agency
IT Venture Tower, Songpa-gu, Seoul, Korea
Corresponding author

Abstract

The evolution to the hyper-connected society reveals itself through the Internet of Things (IoT). In the future service-oriented IoT environment, personal data will be collected, processed and distributed in various ways. The requirements for protection of personal data will also grow. The advanced countries, including EU, USA and Japan, are proactively preparing legal, institutional and technical measures to protect personal data in the IoT environment. This study analyzes the threats of personal data in the IoT environment and the relevant policies of the leading countries. Based on these analyses, this study suggests the policy plans to protect users and the distribution of personal data in the IoT environment which is the foundation of the hyper-connected society.

Keywords: Internet of Things, Privacy, Personal Data protection

1 Introduction

The evolution to the hyper-connected society where people and things are connected with each other over the network reveals itself through the Internet of Things (IoT). IoT is a far-reaching, self-organized network consisting of connected, identifiable and addressable physical things. While the current Machine-to-Machine (M2M) communication is a device-based hardware approach, IoT is a solution-based service-oriented approach. It is the environment where information created by uniquely identifiable things is shared over internet, which is further evolved from the existing wire-communication-based Internet and the mobile Internet [1].

The types of information collected in the IoT environment become diverse. Even if the data collected through IoT are not person-identifiable, combination of the collected data provides the highest ever potential to provide custom services. This technical evolution indicates the increase of risk of new type of violation of personal data or privacy. According to the report (Internet of Things Research Study) published by Hewlett-Packard (HP) in September 2014 [2], 90% of the devices connected to Internet collects at least a piece of personal data, and 70% of the devices use unencrypted network.

This study analyzes the threats to personal data in the IoT environment, and then, compares the policies of the leading countries (USA, EU and Japan). Based on these analyses, this study suggests the policy plans to protect users and the distribution of personal data in the IoT environment which is the foundation of the hyper-connected society.

2 An analysis of threats in the IoT environment over the lifecycle of personal data

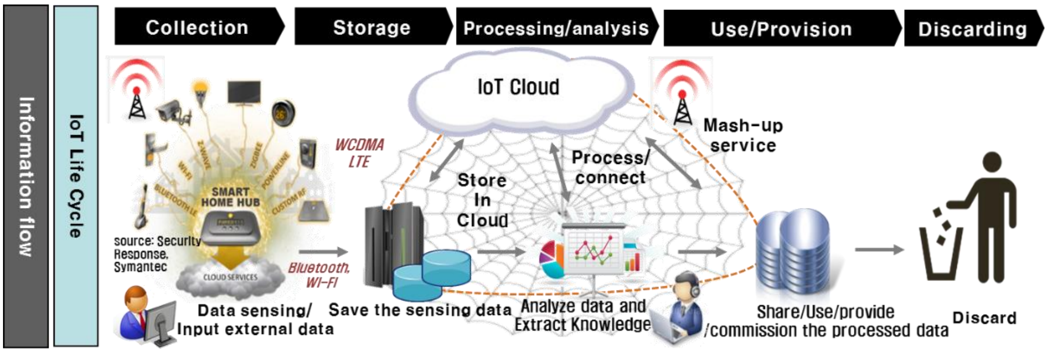

Fig. 1. Personal Data Life Cycle in IoT

[Figure 1] illustrates the lifecycle of personal data distributed/used in the IoT environment. In the IoT environment, the mass data collected through data sensing or input of external data are stored, processed and analyzed with the cloud computing technology and the big data technology.

In the aspect of collection, storage, processing and analysis of personal data, the identification capability of the technically advanced and automated devices and sensors and the data collection capability of the sensors enable collection/storage, profiling and tracing of personal data of many and unspecified individuals, causing a threat to personal data. Processing and analysis of collected data can enable data mining through combination of data from various services and devices, identifying individuals by combining new information with the existing information. Service providers will surely try to receive consents from the data subjects, but it is very hard to acquire consents for the data automatically collected without recognition. Therefore, the way to acquire consent on use of data collected during use of IoT service may become a critical issue.

Threats to the rights of data subjects will also be increased in terms of use and provision of personal data. In the IoT environment, it is difficult for data subjects to realize whether unwanted processing of personal data has occurred, and for the operators to inform data subjects of the processing of data. It is also required to observe principles to protect individual-identifiable data acquired through processing of data. How to observe the principle of collecting minimum data and prohibition of use for other purpose in the self-regulating IoT system will become another issue. One of the major concerns from the viewpoint of data subjects in the IoT environment is that the data processed/analyzed for provisioning of service can be distributed to secondary and tertiary operators, and that they may lose the right to informational self-determination.

3 Analysis of personal data protection policies of leading countries

This study analyzes the technical and institutional aspects of personal data protection in the IoT environment in EU, USA and Japan where relatively active discussion is in progress about the issue.

3-1 Discussion in EU Data Protection Working Party

European Union (EU) is more active than other regions in establishing the IoT security system. The Article 29 Data Protection Working Party (WP29) established under the EU Directive on Data Protection published the opinion titled ‘Opinion 8/2014 on the on Recent Developments on the Internet of Things’ in September 2014 [3].

WP29 suggested 6 privacy and security issues which may occur with the IoT devices. Firstly, there can a lack of control and information asymmetry in distribution of data. In the IoT environment, in order to provide universal services constantly, a large quantity of data is exchanged automatically via inter-device communication. Such data, however, may be too large for the data subjects to examine one by one or to control, resulting in excessive leakage of personal data. Especially in the big data or cloud computing environment, increase of quantity of data makes it difficult for data subjects to know where their data are collected from or sent to, causing an information asymmetry.

Secondly, there can be a problem of quality of the user’s consent on use of data. In the IoT environment, there is a high possibility that users do not recognize the data processed by specific devices. In other words, it is difficult to apply the procedure like the current consent on utilization of personal data to the collection of data by so many IoT devices. As a result, consent on utilization of data in the IoT environment will inevitably be lower quality than that of the current environment. In this regard, WP29 noted that the level of consent on utilization of personal data handled under the existing EU Data Protection Act would not be guaranteed in the future IoT environment.

Thirdly, there can be an inference derived from data and repurposing of original processing. As the quantity of data increases in the IoT environment with combinations of data analysis and cross-matching techniques, there is a possibility that data are provided to third parties beyond the original purpose of collection. Minor data collected via a smart device can be used to infer totally different meaningful information (for example, a driving habit).

Fourthly, there can be an intrusive brining out of behavior and profiling. While various IoT things collect data independently, large quantity of data collected and analyzed can expose habits, behavior or preferences of individuals. As mentioned above, information can be created from minor or anonymous data. Surveillance in the future IoT environment may intrude into home and personal area.

Fifthly, there are limitations on the possibility to remain anonymous when using services. For example, when a wearable device is placed near a data subject, an RF fingerprint is created, enabling tracing of the data subject. This makes it possible to use identities like MAC addresses of useful devices. In other words, collection of MAC addresses of various sensors facilitates creation of RF fingerprint and identity of a specific person, enabling use of data for various purposes, including analysis of location and movement pattern.

Sixthly, there are security risks: security vs. efficiency. In order to expand the encryption space in consideration of security of IoT, it is required to reduce the battery space and to secure the physical efficiency of the sensor. Therefore, there is a difficulty in encrypting IoT sensors and applying automatic security updates.

3-2 Discussion in US FTC

In USA, the Federal Trade Commission (FTC) leads the effort to find the solution for the security problems of IoT. On 19th of November 2013, FTC held a workshop on the ‘Internet of Things: Privacy and Security in a Connected World’. In this workshop, they discussed on how the regulatory authorities, the service providers and the consumers should handle the privacy and security problems in the IoT environment.

Based on the discussions in the workshop, Chairperson Julie Brill of FTC stated, in the address of 14th of March 2014, that device vendors and service providers of IoT need to observe the following 3 principles [4]:

Firstly, the concept of Privacy by Design should be followed: Many IoT devices provide few user interfaces, requiring the service providers to provide products and services in consideration of personal data protection.

Secondly, a robust deidentification of personal data is required: There is a possibility that data are transferred between various devices and services in the IoT environment. Therefore, deidentification of personal data is very important.

Thirdly, an effective transparency is required: Providing prompt, clear, general and highly readable notice facilitates users to understand which data is collected and transferred.

The above principles, however, are not specifically applied to IoT, but were included in FTC's 2012 report titled 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers)'. These principles become more important in the IoT environment [5].

3-3 Discussions in the Japanese Government

The Japanese government expects, in the 'Active Japan ICT Strategy' published in July 2012, that the data market collecting, transmitting and analyzing large amount of various data should grow to dozens of trillions of Yen by 2020 [6]. The Japanese government also published the 'ICT Growth Strategy' in 2013 and the 'ICT Growth Strategy II' in 2014 to actively implement the policy to raise utilization of IoT [7].

Reflecting these policies, active discussion is in progress in Japan on protection of personal data in terms of promotion of utilization of big data collected and created in the IoT environment. The Advanced Communication Network Society Strategy Headquarters set up the 'Personal Data Review Board' in September 2013 to prepare for reflection in the revised Personal Data Protection Act. In June 2013, the Advanced Communication Network Society Strategy Headquarters published the 'Report on the Study on Utilization and Distribution of Personal Data'. The report suggested the following 7 principles for utilization of personal data in a broad sense, which includes individual-identifiable data and deidentifiable data (personal data) collected and distributed in the IoT environment:

① Transparency: Data subjects shall easily access the required data in relation with use of personal data.

② Chance for data subjects to participate: Data subjects shall have the chance to participate in use of their personal data (the right to informational self-determination).

③ Respect for the context of data acquisition: Use of personal data shall be handled within the expectation of the data subject in accordance with the circumstances (context) when the data is provided by the data subject (prohibition of use for other purpose)

④ Minimum data collection: Collection of personal data shall be the minimum required for implementation of the purpose of use.

⑤ Collection with appropriate means: Personal data shall be collected with appropriate means.

⑥ Appropriate safety management measures: Handling of personal data shall accompany with appropriate safety management measures.

⑦ Privacy by Design: Users of personal data shall consider protection of privacy in the overall business cycle, including development of service.

The report also notes that the scope of personal data to be protected shall be based on the identifiability actually determined in accordance with the above-mentioned

7 principles (so called, actual identifiability). For example, the identification data (terminal ID, etc.) of a personal computer or a smartphone is the data used to identify a specific device, but is actually connected with an individual constantly, satisfying the requirement of actual identifiability, and therefore, is considered to be an object of protection. An IP address or a cookie does not always identify a specific device, and hence, is not an object of protection. If it is collected in link with other personal data, it has the actual identifiability. Continuously collected purchase history, rental history, watch history and location data are the objects of protection since they have high identifiability even when they are not linked with other actual identifiability data. The report classifies the sensitive data, such as ideology, religion, belief, ethnic group, criminal record and medical history, as the objects of absolute protection. Whether the financial data or property data can be considered as sensitive data needs a consideration based on the domestic situation in Japan.

4 Conclusion: Result of analysis of the personal data protection policies of leading countries

Characteristics of the policies of the leading countries, such as EU, USA and Japan, are summarized as follows. EU is considering the personal data protection in the IoT environment within the framework of the existing Data Protection Act, and suggests the relevant measures. In USA, FTC holds the workshop to exchange opinion with the relevant industries and the experts, and suggests the direction of personal data protection in the IoT environment. Japan is discussing the issues in the aspect of use and distribution of personal data in the IoT environment, and implements the policies by reflecting the discussion in the revision of the Personal Data Protection Act.

Based on the examination of policies of the leading countries, the following policy considerations are suggested. Firstly, it is required to define the stakeholders in the IoT environment. For example, EU WP29 divides the IoT stakeholders into device manufacturers, social platforms, application developers, other third parties and IoT data platforms.

As mentioned in EU WP 29 report, the key element of IoT is to provide the service in link with cloud computing and big data. Various participants have interests in this process. The ultimate problem of IoT is how to handle personal data provided by data subjects and create added value, but it is required to clearly define the stakeholders. This will become a critical variable in coordinating the interests in the future.

Secondly, it is required to set up the basic principles for handling of personal data in the IoT environment. It is required for the government or a public institution to suggest opinion on which standards and principles should be applied to technical or institutional handling of data while the collected data are transferred along the lifecycle of personal data.

Based on the above policy considerations, it is required to establish the policy guidelines in the aspect of promoting the IoT-related industries and protecting users.

As the IoT industry is expected to be established as a core growth engine of the ICT industry, it is very important to establish the policies applicable to the global environment.

References

[1] Kyoungsik Min, An Analysis of IoT Global market Trend, Internet & Security Issue, *Korea Internet & Security Agency*, (2012), no. 9, 3-33.

[2] http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[3] Opinion 8/2014 on the on Recent Developments on the Internet of Things (Wp29). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/ files/2014/wp223_en.pdf

[4] http://www.ftc.gov/system/files/documents/public_statements/289531/140314fordhamprivacyspeech.pdf

[5] Fujii Hideyuki, *Discussion Trends Privacy Protection of Internet of Things* (IoT), InfoCom Law Report, InfoCom Research, 2014.

[6] Information and Communications Council, Active Japan ICT Strategy, 2012.

[7] www.soumu.go.jp/main_content/000236560.pdf

Received: April 11, 2016; Published: June 2, 2016